MS 404 Insider Threat Program

Effective Date: August 13, 2014
Responsible Office: Office of Safety and Security
Supersedes: New Manual Section

Issuance Memo (8/13/2014)

Insider Threat Program Committee Charter

1.0 Purpose

This policy establishes the Insider Threat Program within the Peace Corps and assigns duties and responsibilities to implement the policy.

2.0 Authorities

Peace Corps Act, 22 U.S.C. 2519; Executive Order 10450; Executive Order 13526; Executive Order 13587; Executive Order 12968; Executive Order 10450; and Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated November 21, 2012.

3.0 Policy

(a) The Peace Corps will maintain an Insider Threat Program to deter, detect, and mitigate insider threats. The Insider Threat Program shall be managed by the Designated Senior Official and shall be consistent with Executive Order 13526 and Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

(b) The Insider Threat Program shall be designed to deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate risks through appropriate insider threat training and response actions.

(c) The Peace Corps will ensure that legal, civil and privacy rights are safeguarded under the Insider Threat Program.

(d) Employees must be trained to be aware of insider threats and how to report them. Employees who have access to or responsibility for classified material should receive appropriate training for the information they are able to access.

(e) Employees must report insider threats, including activities or behaviors which could adversely impact the protection of classified information.

(f) Personnel assigned to support the Insider Threat Program will respond to reports of insider threats and take appropriate response actions.

4.0 Definitions

4.1 ***Classified Information*** means information that has been determined pursuant to EO 13526 or any successor order, EO 12951 or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

4.2 ***Insider*** means any person with authorized access to any Peace Corps resource, including personnel, facilities, information, equipment, networks, or systems.

4.3 ***Insider Threat*** means the threat that an employee will use his/her authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

4.4 ***Insider Threat Response Action(s)*** means activities to ascertain whether certain matters or information indicates the presence of an insider threat, as well as activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of internal offices, such as the Office of Safety and Security or Office of Inspector General, or by outside authorities, such as the Federal Bureau of Investigation.

4.5 ***Employee*** means a person employed by the Peace Corps, whether full-time or part-time, permanent or temporary, and includes for purposes of this policy individuals performing duties as experts, consultants, personal services contractors, and contractors (non-personal services contractors).

4.6 ***Minimum Standards*** means the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs issued by the Presidential Memorandum on November 21, 2012.

4.7 ***Cleared Employee or Official*** means a person who has been granted access to classified information.

5.0 Roles and Responsibilities

5.1 Peace Corps Director

The Peace Corps Director is responsible for establishing and overseeing the Insider Threat Program and taking appropriate actions to ensure that it complies with this Manual Section.

5.2 Associate Director for Safety and Security

The Associate Director for Safety and Security serves as the Designated Senior Official for the Insider Threat Program and is responsible for the implementation, management, and the day-to-day operation of the Insider Threat Program. As the Designated Senior Official, the Associate Director shall:

(a) Ensure that the Insider Threat Program includes and operates in compliance with the Minimum Standards.

(b) Prepare an implementation plan for the Insider Threat Program, report annually to the Director on its performance and make recommendations to the Director regarding the Insider Threat Program.

(c) Establish a process to gather, monitor, integrate, and centrally analyze, and respond to insider threats that are identified through employee reports or through electronic surveillance.

(d) Establish oversight standards to ensure proper handling and use of records and data and to ensure that access to such records and data is restricted to staff who work on the Insider Threat Program. Retain records necessary to complete assessments required by Executive Order 13587.

(e) Initiate appropriate insider threat response actions, including referral of matters to an internal entity, such as the Office of Safety and Security or the Office of Inspector General, or external investigative entities such as the Federal Bureau of Investigation or the Department of Justice.

(f) In consultation with the Office of the General Counsel, ensure that all Insider Threat Program activities are conducted in accordance with applicable laws, whistleblower protections, and civil liberties and privacy policies.

(g) Facilitate oversight reviews by cleared officials designated by the Director to ensure compliance with the Minimum Standards.

(h) Establish the process for insider threat response actions, such as inquiries, to clarify or resolve insider threat matters while ensuring that such response actions are centrally managed by the Insider Threat Program.

(i) Ensure the proper training of staff who support the Insider Threat Program.

(j) Negotiate agreements with the providers of classified data network services to monitor user activity by Peace Corps personnel on the networks in order to detect activity indicative of insider threat behavior by establishing Service Level Agreements (SLA) with the providers. The SLA will outline the capabilities that the provider will employ to identify suspicious user behavior on the secure networks for users both at Peace Corps Headquarters and at external locations. The SLA will also address how that information shall be reported to the Designated Senior Official.

5.3 Information Security Specialist, Office of Safety and Security

The Information Security Specialist for the Office of Safety and Security is the Insider Threat Program Manager and shall be responsible for gathering and integrating relevant information, analyzing the information for indications of possible malicious insider activity, and ensuring that the Peace Corps responds appropriately to all insider threat concerns. The Program Manager shall:

(a) Provide insider threat awareness training, either in-person or computer-based, to all cleared employees within 30 days of initial employment, entry-on-duty, or following the granting of access to classified information, and annually thereafter.

(b) Verify that all cleared employees have completed the required insider threat awareness training.

(c) Establish and promote an internal network site accessible to all cleared employees to provide insider threat reference material, including indicators of insider threat behavior, applicable reporting requirements and procedures, and provide a secure electronic means of reporting matters to the insider threat program.

5.4 Chief Information Officer

The Chief Information Officer will:

(a) Ensure that network banners are employed on unclassified networks, to include government portable electronic devices, to inform consenting users that the network is being monitored for lawful U.S. Government-authorized purposes and can result in criminal, civil and/or administrative actions in accordance with MS 542 and the Rules of Behavior.

(b) Ensure that all employees having access to any Peace Corps unclassified network, including portable electronic devices, sign agreements acknowledging that their activity is subject to monitoring.

(c) Monitor all user activity on unclassified networks for the purposes of detecting activity indicative of insider threat behavior.

5.5 General Counsel

The General Counsel will:

(a) Provide legal advice to offices to assist them in performing their responsibilities under the Insider Threat Program.

(b) Provide counsel regarding operation of the Insider Threat Program to ensure that all insider threat program activities are conducted in accordance with applicable laws regarding privacy and civil liberty policies.

5.6 Office Heads

Heads of offices are responsible for providing the Insider Threat Program Committee, and staff working on the Insider Threat Program regular, timely, and if possible electronic access to information necessary to identify, analyze, and resolve insider threats.

5.7 Insider Threat Program Committee

The Insider Threat Program Committee shall be headed by the Designated Senior Official and shall include members from the Office of the Chief Information Officer, the Office of Safety and Security, the Office of Human Resource Management and the Office of the General Counsel. The Insider Threat Program Committee is responsible for:

(a) Providing oversight of the operation of the Insider Threat Program and making recommendations to the Director on program development, implementation and management.

(b) Approving procedures required by the Minimum Standards or needed to implement this Manual Section.

(c) Advising the Designated Senior Official on insider threat response actions.

5.8 Inspector General

The Inspector General will:

(a) Assign an investigative liaison from the Office of Inspector General to assist the Insider Threat Program Committee with investigations as requested.

(b) At the request of the Insider Threat Program Committee, make referrals of matters to external investigative entities such as the Federal Bureau of Investigation or the Department of Justice.

6.0 Training for the Insider Threat Program Staff

Staff assigned to the Insider Threat Program shall be trained on the subjects specified in the Minimum Standards, including applicable laws and regulations governing privacy and civil liberties; safeguarding of records and data, including the consequences of misuse of such information; and the statutory investigative referral requirements, as well as other policy and statutory requirements that require referrals to an internal entity, such as the Office of Safety and Security or the Office of the Inspector General, or external investigative entities such as the Federal Bureau of Investigation or the Department of Justice

7.0 Access to Information

Peace Corps offices, employees and contractors shall, upon request, provide the Insider Threat Program Committee and staff working on the Insider Threat Program, with regular, timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. If the Office of Inspector General receives a request for access to such information, the Office of Inspector General must determine whether providing access to such information would interfere or compromise an investigation of the Office of Inspector General. The Insider Threat Program Committee will develop and approve procedures and guidelines for access to information that comply with the Minimum Standards.

8.0 Effective Date

The effective date is the date of issuance.